AFFIDAVIT OF J. ALEX HALDERMAN

J. ALEX HALDERMAN, being duly sworn, deposes and says the following under penalty of perjury:

1. My name is J. Alex Halderman. I am a Professor of Computer Science and Engineering and the Director of the Center for Computer Security and Society at the University of Michigan in Ann Arbor, Michigan. I submit this Affidavit in support of Jill Stein's Petition for a hand recount of all ballots in Wisconsin.

2. I have a Ph.D., a Master's Degree, and a Bachelor's Degree in Computer Science, all from Princeton University.

3. My research focuses on computer security and privacy, with an emphasis on problems that broadly impact society and public policy. Among my areas of research are software security, data privacy, and electronic voting.

4. I have authored more than seventy articles and books. My work has been cited in more than 4,700 scholarly publications. I have served on the program committees for thirty research conferences and workshops, and I co-chaired the USENIX Election Technology Workshop, which focuses on electronic voting security. I received the John Gideon Award for Election Integrity from the Election Verification Network, the Alfred P. Sloan Foundation Research Fellowship, the IRTF Applied Networking Research Prize, and the University of Michigan College of Engineering 1938 E Award for teaching and scholarship.

5. I have published peer-reviewed research analyzing the security of electronic voting systems used in Wisconsin, other U.S. states, and other countries. I was part of a team of experts commissioned by the California Secretary of State to conduct a "Top-to-Bottom" review of the

state's electronic voting systems. I have also investigated methods for improving the security of electronic voting, such as efficient techniques for testing whether electronic vote totals match paper vote records.

6. My full curriculum vitae, including a list of honors and awards, research projects, and publications, is attached as Exhibit A.

Context: Cyberattacks and the 2016 Presidential Election

7. The 2016 presidential election was subject to unprecedented cyberattacks apparently intended to interfere with the election. This summer, attackers broke into the email system of the Democratic National Committee and, separately, into the email account of John Podesta, the chairman of Secretary Clinton's campaign. Exhibits B and C. The attackers leaked private messages from both hacks. Attackers also infiltrated the voter registration systems of two states, Illinois and Arizona, and stole voter data. Exhibit D. The Department of Homeland Security has stated that senior officials in the Russian government commissioned these attacks. Exhibit E. Attackers attempted to breach election offices in more than 20 other states. Exhibit F.

8. Russia has sophisticated cyber-offensive capabilities, and it has shown a willingness to use them to hack elections elsewhere. For instance, according to published reports, during the 2014 presidential election in Ukraine, attackers linked to Russia sabotaged Ukraine's vote-counting infrastructure, and Ukrainian officials succeeded only at the last minute in defusing vote-stealing malware that could have caused the wrong winner to be announced. Exhibit G. Countries other than Russia also have similarly sophisticated cyberwarfare capabilities.

9. If a foreign government were to attempt to hack American voting machines to influence the outcome of a presidential election, one might expect the attackers to proceed as follows. First, the attackers might probe election offices (or the offices of election service vendors) well in advance to find ways to break into the computers. Next, closer to the election, when it was clear from polling data which states would have close electoral margins, the attackers might spread malware into voting machines in some of these states, manipulating the machines to shift a few percent of the vote to favor their desired candidate. One would expect a skilled attacker's work to leave no visible signs, other than a surprising electoral outcome in which results in several close states differed from pre-election polling.

The Vulnerability of American Voting Machines to Cyberattack

10. As I and other experts have repeatedly documented in peer-reviewed and state-sponsored research studies, American voting machines have serious cybersecurity problems. Voting machines are computers with reprogrammable software. An attacker who can modify that software by infecting the machines with malware can cause the machines to provide any result of the attacker's choosing. As I have demonstrated in laboratory tests, in just a few seconds, anyone can install vote-stealing malware on a voting machine that silently alters the electronic records of every vote.[1]

11. Whether voting machines are connected to the Internet is irrelevant. Sophisticated attackers such as nation-states have a developed a variety of techniques for attacking non-Internet-connected systems.[2] Shortly before each election, poll workers copy the ballot

[1] A video documenting this result is publicly available at https://youtu.be/aZws98jw67g.

[2] A well known example of this ability, which is known as "jumping an airgap", is the Stuxnet computer virus, which was created to sabbotage Iran's nuclear centrifuge program by attacking factory equipment that was not directly connected to the Internet: https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

design from a regular desktop computer in a government office (or at a company that services the voting machines) and use removable media (akin to the memory card in a digital camera) to load the ballot design onto each machine. That initial computer is almost certainly not well enough secured to guard against attacks by foreign governments. If technically sophisticated attackers infect that computer, they can spread vote-stealing malware to every voting machine in the area. Most voting machines also have reprogrammable software ("firmware") that can in many cases be manipulated well in advance of the election to introduce vote-stealing malware. Technically sophisticated attackers can accomplish this with ease.

12. While the vulnerabilities of American voting machines have been known for some time, states' responses to these vulnerabilities have been patchy and inconsistent at best. Many states, including Wisconsin, continue to use out-of-date machines that are known to be insecure.

13. Procedural safeguards used by Wisconsin and other states to protect their voting equipment are inadequate to guard against manipulation of the election outcome via cyberattack. These inadequate safeguards include tamper evident seals, protective counters, and test decks. Tamper evident seals do not protect against remote electronic attackers, and may not even defend against local attackers.[3] Malware installed on a voting machine can subvert the protective counter by changing its value in the machine's computer memory. Malware can subvert test decks by refraining from cheating when only a small number of ballots have been scanned (as is the case when a test deck is used), or by only cheating at a specified time of day (electronic voting machines typically have internal clocks).

[3] The types of seals commonly used on voting equipment have been shown to be easily defeated in tests. For a review of tamper-evident seal security, see https://www.americanscientist.org/issues/page2/tamper-indicating-seals.

14. The companies that provide and service election equipment for municipalities are another possible target for attackers. An example of such as a vendor is Command Central Elections[4], a small business in Minnesota that provides voting machines to approximately 1000 municipalities in Wisconsin.[5] In many municipalities, Command Central is responsible for updating voting machine software and programming ballot designs prior to the election. Such companies provide an attractive target for attackers, since compromising their computer systems would allow an attack to spread to voting machines over much of the state. An attack on Command Central could affect election in hundreds of jurisdictions statewide by altering the software or election media in malicious ways that could go detected absent a manual examination of the ballots.

Examining the Paper Record Is the Only Way to Ensure the Integrity of the Result

15. Paper ballots are the best and most secure technology available for casting votes. Optical scan voting allows the voter to fill out a paper ballot that is scanned and counted by a computer. Electronic voting machines with voter-verified paper audit trails allow the voter to review a printed record of the vote he has just cast on a computer. Only a paper record documents the vote in a manner that cannot later be modified by malware or other forms of cyberattacks.

16. One explanation for the results of the 2016 presidential election is that cyberattacks influenced the result. This explanation is plausible, in light of other known cyberattacks intended to affect the outcome of the election; the profound vulnerability of American voting machines to cyberattack; and the fact that a skilled attacker would leave no outwardly visible evidence of an attack other than an unexpected result.

[4] http://ccelections.com/

[5] http://elections.wi.gov/elections-voting/voting-equipment/voting-equipment-use

17. The only way to determine whether a cyberattack affected the outcome of the 2016 presidential election is to examine the available physical evidence—that is, to count the paper ballots and paper audit trail records, and review the voting equipment, to ensure that the votes cast by actual voters match the results determined by the computers.

18. More than 70% of American voters, and all Wisconsin voters, have their votes recorded on some form of paper, which provides permanent evidence of their intent in the event of a post-election recount. Wisconsin's paper vote records will not serve as a defense against cyberattacks unless they are inspected by human beings.

Recounting Ballots With Optical Scan Tabulators Will Not Reliably Detect Manipulation

19. For ballots cast through optical scanners, a manual recount of the paper ballots, without relying on the electronic equipment, is necessary to reliably detect possible hacking. Using optical scan machines to conduct the recount, even after first evaluating the machines through a test deck, is insufficient to detect potential cyberattacks. Attackers intending to commit a successful cyberattack could, and likely would, create a method to undermine any pre-tests.[6]

20. If the scanners were attacked by infecting them with malware, such malware might still be active in the scanners during the recount. Recounting the ballots using an infected scanner would likely yield the same results as the original count, despite the results being wrong.

21. If attackers managed to compromise the count during election day but in a manner that did not persist on the machines, machine recounts would still be insufficient. Attackers who were able to infect the machines before the election likely would be able to attack them again, perhaps using the same methods, prior to the recount. The dates and the procedures of the

[6] Volkswagen used a similar strategy to conceal the way its circumvent EPA emissions tests: http://www.reuters.com/article/us-volkswagen-emissions-audi-idUSKBN1370Q3

recount are widely publicized, so attackers would know when to strike. This would result in the scanners producing the same incorrect results when the ballots were scanned again.

22. In contrast to machine recounts, a manual recount, where the paper ballots are inspected by humans, can reliably detect any cyberattack that might have altered the election outcome on the optical scanners. A manual recount is the best way, and indeed the only way, to ensure public confidence that the results are accurate, authentic, and untainted by interference.

23. Manual recounts are not necessarily more time-consuming than recounting using optical scanners, particularly when only one race is being counted. A manual recount focuses on a single contest, and human observers typically proceed by sorting the ballots into stacks according to the chosen candidate and then counting the ballots in each stack. This is an efficient and straightforward process. If scanners are used, the scanners must be programmed and tested, new removable media must be located and programmed, and the ballots must be fed into the scanner by humans. These steps are not necessary when hand counting is used.

24. The paper ballots used in Wisconsin can be counted much more easily and reliably than the punched card paper ballots that were recounted in Florida during the 2000 presidential election. Punched card ballots are fragile, so each time they are counted, the record of voters' intent may be inadvertently altered. They are also difficult to interpret, sometimes requiring a magnifying glass to discern whether the voter intended to make a mark. Wisconsin's optically scanned paper ballots are a completely different technology. They create a persistent and readily interpretable record of voters' intent that does not suffer from these problems, and they can be counted efficiently and accurately in a manual recount.

25. A manual recount will also set a precedent that will provide an important deterrent against cyberattacks on future elections. By performing a rigorous recount now in a method that would detect cyberattacks affecting the outcome (that is, a manual recount), we send a strong signal to attackers that any future computer-based tampering efforts are likely to be caught.

This affidavit was executed on the 28th day of November, 2016 in Newtown, Pennsylvania.

J. ALEX HALDERMAN

Sworn to before me this 28th day of November, 2016.

Notary Public

COMMONWEALTH OF PENNSYLVANIA
NOTARIAL SEAL
Swapnil Patel, Notary Public
Middletown Twp., Bucks County
My Commission Expires Aug. 5, 2020
MEMBER, PENNSYLVANIA ASSOCIATION OF NOTARIES

My Commission Expires: 08-05-2020